S: 11 Sep 2007
DAMI-CDS-SO
28 Aug 2007

MEMORANDUM FOR All HQDA SSO Supported Security Managers

SUBJECT: Continuing Security Awareness Program

1. Enclosed you will find Continuing Security Awareness Program training slides.

2. As prescribed in DoD 5105.21-M-1, all persons granted SCI access will be advised at least annually of their continuing security responsibilities.

3. In order to receive credit for training, all personnel are required to turn in their signed certificate and the "Watched DVD Only No Foreign Travel" form to their Security Manager.

4. Security Manager's will ensure that all SCI indoctrinated personnel assigned/attached to their organization complete Continuing Security Awareness Program training no later than 24 Sep 07. If an individual is on leave, then it will be completed upon their return. Additionally, Security Manager's will forward the names and dates training was completed to SSO DA, Personnel Security Branch in a roster format, no later than 28 Sep 07. We do not want printed certificates.

5. Point of contacts for HQDA SSO are, Personnel Security Branch at 695-2758, 695-6663, and Physical Security 703-697-6349/3226.

U.S. Army Special Security Office

CONTINUING SECURITY AWARENESS PROGRAM

OVERVIEW

- FOREIGN INTELLIGENCE THREAT
- SECURITY RISKS WITH NEW TECHNOLOGY
- EMPLOYEE OUTSIDE ACTIVITIES
- FOREIGN TRAVEL/CONTACTS
- CLASSIFICATION AND CONTROL MARKINGS
- PREPUBLICATION REVIEW REQUIREMENT
- JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS)

FOREIGN INTELLIGENCE THREAT

1. THE FOREIGN INTELLIGENCE THREAT BRIEF (FITB) addresses efforts by Foreign Intelligence Services (FIS), foreign commercial enterprises, foreign terrorists, or foreign computer intruders to acquire U.S. classified, sensitive, or proprietary information or material, and the unauthorized disclosure of such information or material to foreign sources.

2. The FITB discusses the Source of the Threat, OPSEC, Type of Information Being Targeted, the Insider Threat, Volunteer Spies, Personal Security Indicators that would indicate Improper or Suspicious Activity, and the Technical / Non-HUMINT Threat.

3. Think about it! How does the FIS Agent gather information about you or your organization? Your detailed

FOREIGN INTELLIGENCE THREAT

3. … your's or family members' personal web sites such as My Space or Facebook Pages; conversations with fellow commuters about the frustrations of the day soon turn into discussions about where you work, what you do, family, the cost of housing, kids college, and other financial woes; cell phone conversations with clients or co-workers discussing work, setting up meetings, going over slides to correct errors; organizational websites highlighting new technology and specifications, news releases, deployment photos, social calendars, and so much more is collected to be used against us.

4. How much did you disclose? What has the FIS agent gained? Who have you endangered? What damage have you caused? When the puzzle of information is put together and the dots connected, you may have disclosed

FOREIGN INTELLIGENCE THREAT

4. … placed your family, co-workers, yourself, Troops overseas, and your Nation in Grave Danger! The damage you have caused is irreparable and the devastation can be seen in the body bags and grave sites!

5. You can protect yourself and your organization by maintaining situational awareness, practicing OPSEC, and staying educated by using the resources available within the Intel Community. Unclassified information on the current Foreign Intelligence Threat, and other CI publications can be found on the Office of the Director National Intelligence / Office of the National Counterintelligence Executive webpage http://www.ncix.gov/archives/index.html

6. The following invaluable resources are located in the NCIX

FOREIGN INTELLIGENCE THREAT

6a. ...intel threat against Corporations is the, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage, 2005

http://www.ncix.gov/publications/reports/fecie_all/FECIE_2005.pdf

b. CI Reader: An American Revolution into the New Millinium Volumes I-IV

http://www.ncix.gov/issues/CI_Reader/index.html

7. Additional guidance is posted on these IC and Security-Related Sites:

a. Economic Espionage

http://www.fbi.gov/hq/ci/economic.htm

b. Research & Technology (RPT) Program

http://www.infragard.net/

FOREIGN INTELLIGENCE THREAT

e. Office of the Director of National Intelligence

http://www.dni.gov/testimonies/20060228_testimony.htm

f. DSS Industrial Security Counterintelligence

https://www.dss.mil/portal/ShowBinary/BEA%20Repository/new_dss_internet//isp/count_intell/count_n_sec_count_meas.html

8. **The key to reducing the Foreign Intelligence Threat is to Practice and Remember OPSEC! National Security is everybody's business!**

SECURITY RISKS WITH NEW TECHNOLOGY

Mass Storage

Miniaturization

Imaging Technology

Wireless Technology

Advances

THE FOLLOWING 8 SLIDES DEPICTS DEVICES THAT ARE CAPABLE OF ELECTRONICALLY GATHERING/COPYING INFORMATION

SECURITY RISKS WITH NEW TECHNOLOGY

New Technology poses new threats to security, not limited to Computer Security Next Generation Devices, new devices and miniaturization.

Pen Drive

Thumb Drive

Shoaib Amin / AP

Security Risks w
New Technolog

- **The problem is rea**
- **Stolen military dat**

for sale in Afghanist

Despite crackdown, computer drives found with names of HUMINT sources.

- Memory sticks (Thumb Drives) like these, on sale at the bazaar outside the U.S. military base in Bagram, were found to contain U.S. intelligence data.

SECURITY RISKS WITH NEW TECHNOLOGY

Imaging Devices

USB Memory Watch

SECURITY RISKS WITH NEW TECHNOLOGY

Miniaturization

Casio Watch Camera:

Casio Audio Recorder:

MP3 Devices

SECURITY RISKS WITH NEW TECHNOLOGY

New Video Devices

New Audio Recorders with USB connectivity

SECURITY RISKS WITH NEW TECHNOLOGY

The Mother Lode

Terapin Mine

Other USB Gizmos

SECURITY RISKS WITH NEW TECHNOLOGY

Integrated Devices

SECURITY RISKS WITH NEW TECHNOLOGY

Integrated Devices

SECURITY RISKS WITH NEW TECHNOLOGY

Defense

- Educate Users!
- Work closely with System Administrators and Information Systems Security Officers (ISSO).
- Inquire about technical details of products purchased.
- Pass information on to those who do Entry / Exit inspections.
- Conduct periodic system inspections.
- Be aware of possible risks and pay attention to those around you.

Bottom Line

Don’t assume the device is authorized in the facility.
Contact the Security Office if you have any questions.
Inquire about technical details of proposed purchases before ordering items.

EMPLOYEE OUTSIDE ACTIVITIES

1. Potential conflicts with an individual's responsibility to protect SCI material may arise from outside employment or other outside activity from contact or association with foreign nationals.

2. In cases where such employment or association has resulted in a suspected or established compromise of SCI, the local SCI security official and supporting CI activity must be advised immediately.

3. Involvement in non-U.S. government employment or activities that raise potential conflicts with an individual's responsibility to protect classified information is of security concern and must be evaluated by an SCI security official to determine whether the conflict is of such a nature that SCI access should be denied or revoked.

4. Individuals who hold or are being considered for SCI access approval must report in writing to the local SCI security official any existing or contemplated outside employment or activity that appears to meet the criteria listed below:

EMPLOYEE OUTSIDE ACTIVITIES (CONT'D)

a. Employment that must be reported includes compensated or volunteer service with any foreign national; with a representative of any foreign interest; or with any foreign, domestic, or international organization or person engaged in analysis, discussion, or publication of material on intelligence, defense, or foreign affairs.

b. Continuing association with foreign nationals must be reported.

c. When outside employment of activity raises doubt as to an individual's willingness or ability to safeguard classified information, he/she will be advised that continuing that employment or activity may result in withdrawal of SCI access, and be given an opportunity to discontinue. If the individual terminates the outside employment or activity of security concern, his or her SCI access approval(s) may be continued, provided this is otherwise consistent with national security requirements.

FOREIGN TRAVEL/CONTACTS

1. Personnel w/ SCI access who plan official or unofficial foreign travel will:

a. View the Foreign Travel Brief, Expect the Unexpected, Defensive Tactics for a Safe Trip Abroad, put out by DIA which is posted on the SSO Unclassified Website at the following link: http://www.dami.army.pentagon.mil/offices/dami-cd/sso/travel.asp Click on this link and follow the instructions.

(1). For the purpose of this training: please watch the video and follow instruction 2 (a), which tells you to print the pdf file "Watched DVD only No Foreign Travel "and fax the signed completed form to the Unclassified Fax for SSO DA at 703-697-3466 (DSN 227)!

b. Report anticipated foreign travel to immediate supervisors or local SCI security officials (Security Manager) by filling out the Foreign Travel Brief form, located in the above mentioned SSO Unclassified Website, which states: the dates of travel, the country (ies) you will be visiting, and the date you received your Foreign Travel Brief.

c. Supervisors will ensure personnel become knowledgeable of threat conditions, monitor the itinerary from a safety point-of-view, and follow-up on security-related issues. Current travel warnings and local customs are available for most foreign countries on the State Department Website: http://travel.state.gov/travel/cis_pa_tw/tw/tw_1764.html

FOREIGN TRAVEL/CONTACTS (CONT'D)

2. SCI indoctrinated personnel must protect themselves against cultivation and possible exploitation by foreign nationals who are or may be working for foreign intelligence services and to whom they might unwittingly provide sensitive or classified national security information.

3. Persons with SCI access have a continuing responsibility to report, within 72 hours, to their immediate supervisor or local SCI security official all contacts:

   a. That are of a close, continuing personal association, characterized by ties of kinship, affection, or obligation with foreign nationals. Casual contacts and associations arising from living in a community normally need not be reported.

   b. In which illegal or authorized access is sought to classified, sensitive, or proprietary information or technology, either within or outside the scope of the employee's official activities. Personnel should be skeptical of requests for information that go beyond the bounds of innocent curiosity or normal business inquiries.

FOREIGN TRAVEL/CONTACTS (CONT'D)

d. With, or invitations from, foreign government officials except as stated in (1) and (2) below:

(1) Unless specifically approved by the appropriate SIO, SOIC, or designee, DoD SCI-Indoctrinated personnel will not initiate contact with foreign government representatives, accept invitations to attend any official or social foreign function, or extend reciprocal invitations.

(2) DoD personnel whose official duties require them to deal officially and socially with foreign nationals must limit their contact and association to the requirements of their duties.

4. Failure to report foreign contacts, as required above, may result in reevaluation of eligibility for continued SCI access. This does not imply that an individual will automatically be subject to administrative action if he/she reports questionable contacts or associations.

5. These instructions are not intended to inhibit or discourage contact with foreign nationals. They are meant to

CLASSIFICATION & CONTROL MARKINGS

The Authorized Classification and Control Markings Register provides seven categories of information

US CLASSIFICATION//NON-US CLASSIFICATION//SCI CONTROL SYSTEMS AND SUB-CATEGORIES//FOREIGN GOVERNMENT INFORMATION//DISSEMINATION CONTROLS//NON-INTELLIGENCE COMMUNITY MARKINGS//DECLASSIFICATION DATE MARKING

… and here is an example of a US-originated classification line with instructions.

Conspicuously place the classification line at the top and bottom of each page; it must be in uppercase with exception of the word "and" in the REL TO marking. A double slash separates categories; use only the categories that apply to the document. When necessary, break the line after a punctuation mark. Mark unclassified documents when transmitted over a classified system or when they contain dissemination controls, such as FOUO

Separate Dissemination Control markings with a comma-no space after the comma. List in order shown in markings register.

In the REL TO markings, always list USA first, followed by other countries in alphabetical trigraph order. Use ISO 3166 trigraph country codes; separate trigraphs with a comma and a space—no comma before or after "and".

The word "and" is the only word in lowercase in the marking system.

TOP SECRET//HCS/COMINT-GAMMA/TK//FGI CAN GBR//RSEN,ORCON,REL TO USA,CAN and GBR//SAR//X5

Identify the SCI control systems and subsystems.

Use a single slash (no space) to separate SCI control systems.

Identify source of FGI in a US-originated document. Use FGI + trigraph country code in alphabetical order, separated by single space.

Use numerical date exemption code, or MR, as appropriate for document. Limited to one entry. Must use X5 if document contains FGI.

Use a hyphen (no space) between the SCI control system identifier (e.g., COMINT and the SCI subsystem (e.g. GAMMA).

Separate multiple Non-Intelligence Community markings with a comma—no space after the comma.

Precedence Order and Authorized Portion Markings

1.US Classification
TOP SECRET (TS)
SECRET (S)
CONFIDENTIAL (C)
UNCLASSIFIED (U)

2. Non-US Classification
(//CAN S)
Example: Canadian Secret Information

3. SCI Control System/Subsystem
HCS (HCS)
SPECIAL ACCESS REQUIRED-[nickname] (SAR-NM)
BYE (BYE)
SENSITIVE INFORMATION (SINFO)
COMINT (SI)
GAMMA (G)
TALENT KEYHOLE (TK)

4. Foreign Government Information
Decl block shows "Source Marked OADR"; Document contains Restricted Data, FRD.

5. Dissemination Control Markings
RSEN
FOUO
ORCON
+ SAMI
+ IMCON
NOFORN
PROPIN
Authorized for Release to.. (REL TO) USA/[ALPHABETICAL TRIGRAPH] EYES ONLY

6. Non-Intelligence Community Markings
(RS)
(FOUO)
(OC)
(SAMI)
(IMC)
(NF)
(PR)
+ (Reserved for other countries and international org—NATO, BWCS, CWCS, (EYES)

7. Declassification Information
Date (YYYYMMDD)
X1 thru X8 or EO 12958 (X5 takes priority)
MR – Use "MR" when – based on specific event; COUNTRY
Decl is

PREPUBLICATION REVIEW REQUIREMENT

1. Security Review Process (Prepublication Review). DoD SCI-indoctrinated personnel are encouraged to participate as speakers in recognized forums and to submit professional papers. Such participation encourages the exchange of information and promotes professional growth.

2. Prior to public disclosure in any form, an SCI-indoctrinated or debriefed individual will submit for security review all material intended for disclosure that may contain SCI or SCI-derived information. Submit the material to the Department or Agency that last authorized the individual's access to such information. Review action must start without delay; an initial reply to the author must be made within 30 days.

a. The SCI prepublication review in no way absolves an individual from following the requirements of DoD Directive 5230.9, "Clearance of DoD Information for Public Release," or other regulations requiring certain military/DoD persons to submit material for review prior to public release.

b. The SCI security officer receiving the material will make an initial review and coordinate the review as required. If a determination cannot be made initially as to whether SCI is involved, the material will be forwarded through SCI channels to Command, Defense

PREPUBLICATION REVIEW REQUIREMENT (CONT'D)

3. All proposed public statements on information derived from SCI or concerning SCI operations, sources, or methods must be reviewed and approved before release by the appropriate SOIC or designee.

4. Resumes or applications for employment which detail technical expertise gained through government employment in classified or sensitive programs must be written in an unclassified context even if the potential employer is known to be a cleared defense contractor. A security review should be requested to resolve questions or concerns regarding possible classified content prior to submission to a potential employer. The following statement is appropriate for use in resumes or applications regarding clearance status when seeking employment with an organization involved in classified programs:

CLEARED FOR TOP SECRET INFORMATION AND GRANTED ACCESS TO SENSITIVE COMPARTMENTED INFORMATION BASED ON SINGLE SCOPE BACKGROUND INVESTIGATION COMPLETED ON (DATE).

5. The individual's servicing SCI security official can provide SSBI completion dates and case control numbers. Do not

PREPUBLICATION REVIEW REQUIREMENT (CONT'D)

6. The local SCI security official will establish local written procedures or security reviews or pre-publication reviews. The requirements for security review and prepublication review will be part of the annual security education program. The local SCI security official will ensure that proper local coordination has been effected with the appropriate government agency public affairs or information office to ensure that a prepublication review has been conducted for any public releases that may possibly contain SCI.

JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS)

1. Effective 14 Feb 05, JPAS is the Army's system of record to determine clearance eligibility and current command access level. This change is necessary and desirable in order to provide a single location to input, maintain and retrieve eligibility and access data on all DoD personnel.

2. Account Managers will ensure that all personnel with access to JPAS have received the appropriate live or online training prior to being granted system access.

3. SSO/Security Manager (SM) will create a relationship with each individual that they are responsible for. Every individual must be owned by someone in order for JPAS notifications (adjudications, suspensions, etc) to be transmitted to owners and servicing offices. To determine what type of relationship should exist, use the following guidelines:

JOINT PERSONNEL ADJUDICATION SYSTEM (JPAS) (CONT'D)

a. SSOs will take an "owning" relationship of all SCI cleared personnel that are in their SCI billets by becoming their SCI Security Management Office (SMO).

b. SSOs will take "servicing" relationship of all SCI personnel that they are providing support to when the individual's SCI billet is held by another command/organization.

c. SMs will take an "owning" relationship of all personnel within their command/unit by becoming their non SCI SMOs. This will provide local SMs/Commands/Units with visibility of the status of all of their personnel. It will also cause initial questions regarding clearance issues to be directed to the local SM.

d. SMs will take a "servicing" relationship of all personnel that they do not "own" but for whom they provide supporting services to. (This may include Consolidated Security Offices that provide final transmission of Personnel Security Investigation (PSI) forms and/or maintaining official security records.)

CERTIFICATE OF TRAINING

This is to certify that I, _____,
have completed the
TYPED/PRINTED NAME

Continuing Security Awareness Program Training.

_____ _____
SIGNATURE **DATE**

(Please give this certificate to your Security Manager upon completion of training).